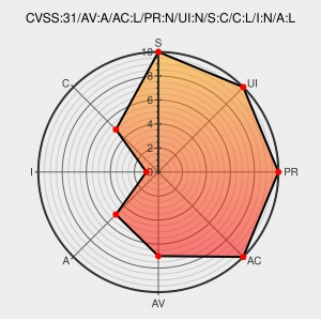
# CVE-2021-21367

Published on: 03/12/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:57 PM UTC

**CVE-2021-21367** - advisory for GHSA-5p3g-j69g-w2mq

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Switchboard Bluetooth Plug from Elementary contain the following vulnerability:

Switchboard Bluetooth Plug for elementary OS from version 2.3.0 and before version version 2.3.5 has an incorrect authorization vulnerability. When the Bluetooth plug is running (in discoverable mode), Bluetooth service requests and pairing requests are automatically accepted, allowing physically proximate attackers to pair with a device running an affected version of switchboard-plug-bluetooth without the active consent of the user. By default, elementary OS doesn't expose any services via Bluetooth that allow information to be extracted by paired Bluetooth devices. However, if such services (i.e. contact list sharing software) have been installed, it's possible that attackers have been able to extract data from such services without authorization. If no such services have been installed, attackers are only able to pair with a device running an affected version without authorization and then play audio out of the device or possibly present a HID device (keyboard, mouse, etc...) to control the device. As such, users should check the list of trusted/paired devices and remove any that are not 100% confirmed to be genuine. This is fixed in version 2.3.5. To reduce the likelihood of this vulnerability on an unpatched version, only open the Bluetooth plug for short intervals when absolutely necessary and preferably not in crowded public areas. To mitigate the risk entirely with unpatched versions, do not open the Bluetooth plug within switchboard at all, and use a different method for pairing devices if necessary (e.g. `bluetoothctl` CLI).

CVE-2021-21367 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **elementary** - **switchboard-plug-bluetooth** version **>= 2.3.0, < 2.3.5**

CVSS3 Score: 8.1 - HIGH

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| ADJACENT_NETWORK | LOW | NONE | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |

| | | | |
|---|---|---|---|
| UNCHANGED | HIGH | HIGH | NONE |

## CVSS2 Score: 4.3 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| ADJACENT_NETWORK | MEDIUM | NONE |

| Confidentiality Impact | Integrity Impact | Availability Impact |
|---|---|---|
| PARTIAL | PARTIAL | NONE |

## CVE References

| Description | Tags | Link |
|---|---|---|
| [SECURITY] Fedora 32 Update: switchboard-plug-bluetooth-2.3.5-1.fc32 - package-announce - Fedora Mailing-Lists | lists.fedoraproject.org text/html | FEDORA FEDORA-2021-7d55c00267 |
| [SECURITY] Fedora 34 Update: switchboard-plug-bluetooth-2.3.5-1.fc34 - package-announce - Fedora Mailing-Lists | lists.fedoraproject.org text/html | FEDORA FEDORA-2021-6210be0100 |
| [SECURITY] Fedora 33 Update: switchboard-plug-bluetooth-2.3.5-1.fc33 - package-announce - Fedora Mailing-Lists | lists.fedoraproject.org text/html | FEDORA FEDORA-2021-3dedd41a06 |
| Merge pull request from GHSA-5p3g-j69g-w2mq · elementary/switchboard-plug-bluetooth@86500e6 · GitHub | github.com text/html | MISC github.com/elementary/switchboard-plug-bluetooth/commit/86500e645a907538abafe5225b67cc12c03e7645 |
| Incorrect Authorization in switchboard-plug-bluetooth · Advisory · elementary/switchboard-plug-bluetooth · GitHub | github.com text/html | CONFIRM github.com/elementary/switchboard-plug-bluetooth/security/advisories/GHSA-5p3g-j69g-w2mq |
| Release switchboard-plug-bluetooth 2.3.5 Released · elementary/switchboard-plug-bluetooth · GitHub | github.com text/html | MISC github.com/elementary/switchboard-plug-bluetooth/releases/tag/2.3.5 |



## Related QID Numbers

281515 Fedora Security Update for switchboard (FEDORA-2021-7d55c00267)

281516 Fedora Security Update for switchboard (FEDORA-2021-3dedd41a06)

281517 Fedora Security Update for switchboard (FEDORA-2021-6210be0100)

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Elementary | Switchboard Bluetooth Plug | All | All | All | All |
| Operating System | Fedoraproject | Fedora | 32 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Fedoraproject | Fedora | 33 | All | All | All |

cpe:2.3:a:elementary:switchboard_bluetooth_plug:*:*:*:*:*:elementary_os:*:*:

cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:33:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→